## Cognito® platform software update

In September 2020, the Vectra® X-series appliances and S-series sensors were updated to Cognito® software release Version 6.1.

The Version 6.1 release introduces a new System Health dashboard, vSensor support for Hyper-V environments, and a number of enhancements to network and O365 detections. On the Recall side there are new Cobalt Strike Malleable Custom Models and a NetLogon visibility dashboard. Cognito® platform enhancements and bug fixes are also included in this release.

## New features

### *System Health Dashboard*

COGNITO **DETECT**

Version 6.1 introduces a new System Health dashboard, a single-pane view in the Detect UI where you can view all major aspects of your Cognito platform's system health. From the System Health dashboard, you can quickly assess:

- Sensors: Determine which sensors are forwarding, not forwarding, or still need to be paired.
- System Info: Get information on disk and memory usage, network interface status, power supplies and general system status.
- External Connectors: Identify misconfigurations, connectivity errors, Lockdown status and find other external connector integrations to enable.
- Product Deployments: Make sure your Recall and Stream deployments are healthy, metadata is flowing, and your licenses are up to date.

Pin the System Health dashboard up in your operations center to keep a watchful eye on your Cognito platform. The System Health dashboard data is updated automatically every five minutes. The Update Now button can be used as necessary to refresh between update intervals.

**Please note:** If you plan to keep the Health Dashboard page up, be sure to enable Auto-Refresh Pages in the General tab on Detect's Settings page.

### *Hyper-V vSensor*

COGNITO **DETECT**

Version 6.1 introduces support for Hyper-V vSensor to provide deeper visibility into Hyper-V deployments. The Hyper-V VSensor image can be downloaded from the Cognito UI under the "Manage -> Sensors" page. Hyper-V sensor can be deployed with 2 or 4 cores to monitor of 500 Mbps or 1 Gbps traffic, respectively.

### *Update to Understanding Vectra AI Documentation*

Version 6.1 includes an update to the Understanding Vectra AI guide that include information about all Detect for Network and Detect for O365 detections.

### *Cobalt Strike Malleable Custom Models*

COGNITO **RECALL**

Cobalt Strike is used by Threat Actors globally. Malicious Actors are always looking for new ways to hide their activity and blend in with normal traffic. One of the methods is to make use of the extensive Malleable profiles available for Cobalt Strike, these profiles allow the C2 tunnel to emulate one of multiple pieces of malware and can dynamically alter its behavior during operation. Vectra Threat Intelligence have developed a collection of Custom Models designed to match the behavior of the profiles available for Cobalt Strike. These searches match the User Agents specific to each profile, and then based on the HTTP Method, the search can then match on multiple patterns from the profile.

These custom models will drive high fidelity, low noise detections, so we will be deploying these detections as enabled by default for all Cognito Recall Customers. If you would not like to receive these notifications, you can disable them easily by navigating to “Manage” -> “Custom Models”, search for “Cobalt Strike”, and then deactivate the custom model within the edit dialog.

### *NetLogon Visibility Dashboard*

COGNITO **RECALL**

A serious CVE was recently reported which enables an attacker to gain Domain Admin privileges by exploiting a vulnerability in how Windows Server OS handles the NetLogon RPC protocol.

The attacker can forge their identity in a password reset event thereby enabling them to reset any password including those of Domain Controllers. It is not required that the attacker have any level of domain credential already - once they can emit traffic to the network, they can exploit this vulnerability. This enables an attacker to elevate permissions from anywhere within the network to Domain Admin quickly and easily.

Vectra’s Behavioral detections driven by strong Artificial Intelligence gives you cover even without any CVE announcement, but we wanted to offer a way for you to investigate this issue directly. We have created a simple dashboard which will show you only the specific hosts which have performed the activity associated with this exploit and will enable the user to quickly drill down on the activity of these hosts.

## Detections

COGNITO DETECT COGNITO DETECT for Office 365

Vectra constantly evaluates detection algorithm coverage and efficacy using opt-in metadata and direct user feedback, which drives targeted enhancements in our algorithms. We encourage your feedback via the Vectra user community.

### *Enhancement to Hidden HTTP Tunnel and Hidden HTTPS Tunnel*

In this release, the coverage provided by the Hidden HTTPS and HTTP Tunnel detections has been enhanced to provide broader coverage for relevant attack behaviors allowing the opportunity for analysts to stop an attack in the earliest stage. Included in the expanded coverage is the ability for the Hidden HTTPS Tunnel detection to alert on DNS over HTTPS (DoH) tunnels which can be run by advanced attack tools like Cobalt Strike.

### *Enhancement to RPC Targeted Recon*

In this release, the coverage provided by the Targeted RPC Recon detection has been enhanced to cover a wider range of reconnaissance commands allowing for analysts to see more steps of an attack progression allowing them to better respond. In addition, coverage related to reconnaissance from new machines in the environment, like attacker drop boxes, has also been improved.

### *Enhancement to O365 DLL Hijacking Activity*

In this release, the coverage provided by the DLL Hijacking Activity detection has been increased to alert on infection activity related to .so and .dylib binaries allowing for more opportunities to find cloud to endpoint pivots. In addition to the coverage expansion, alerts related to normal developer activity have been reduced.

### *Enhancement to O365 Exfil Before Termination*

In this release, the collection window considered in the collection phase has been expanded to 30 days to provide more complete visibility into actions taken by employees prior to departure. In addition to the collection phase expansion, coverage has been expanded to include termination operations performed by Federated Software.

### *Update to Vectra Threat Intelligence Curation*

The daily curation of domains and IPs tracked in Vectra Threat Intelligence and alerted on in Vectra Threat Intel Mach has been updated to more aggressively remove inactive indicators. This change increases the relevance of the report indicator matches and allows analysts to focus on the most current known threats in their environment.

### *Notice to O365 Detect Beta Customers*

In 6.0, Detect for O365 began to process AD sign-on logs. These logs contain rich information about sign-on events in Azure AD authenticated cloud environments. The existing O365 Suspicious Sign-On is planned to begin leveraging these logs in the 6.2 release, increasing its effectiveness in finding stolen accounts. Customers with O365 sensors created during the Beta must be re-consented in order to continue to receive O365 Suspicious Sign-On alerts.

### Detection Deprecation

Attackers may attempt to create a Rouge DC server to progress their attack. Historically, this behavior was covered by the Kerberos Server detection but the recently release RPC Targeted Recon was designed as a replacement and expansion of coverage for this type of attack The Targeted RPC Recon monitors for anomalous usage of DC data replication commands that would allow an attacker to create a Rouge DC server. Given the marked improvement of the Targeted RPC Recon approach the Kerberos Server detection is being deprecated

- Kerberos Server will be deprecated in Version 6.2

### X24 Platform End-of-Life Notice

The X24 hardware platform will be EOL on 30th September 2021.

After the 30th September 2021, Vectra will no longer support:

- Software upgrades for X24 appliances.
- Software upgrades for brain appliances where an X24 sensor is paired.
- Hardware replacements for X24 appliances or their components.

Please contact your Vectra account team to discuss future options for replacing affected X24 hardware prior to the 30th September 2021 date.

### Security updates

This release contains several software updates to harden the security of X-series appliances and S-series sensors.

### Bug fixes

*CS-4379 – Slow UI performance during SQL re-indexing*

Addresses issue where users may experience UI slowness during SQL re-indexing due to the calculation of group membership counts in the Groups dropdown filter on the Manage Triage Filters page.

**Please Note:** To address CS-4379, the UI will no longer compute group membership counts while SQL indexing is in progress. During this time, groups listed in the Groups dropdown filter will show no members. Once SQL indexing has completed, group membership counts will again show accurate member counts.

*CS-4342 – Stream Kafka producer does not save prepend correctly*
Corrects issue where the value in the prepend field is not saved correctly when using Kafka producer for Cognito stream.

*CS-4208 – Recall CSV export does not match Kibana timestamps*
Fixes and issue where Recall CSV data export shows a one-hour timestamp offset.

*CS-4381 – Backup test command test terminates ssh session*
Resolves issue where the 'backup test' command terminates the user's ssh session when backup target is not reachable.
*CS-4245 – PAA triage not working as expected*
Resolves issue where triage of Privilege Anomaly: Unusual Insider detection does not result in a filtering match when account and service are applied in matching conditions.

*CS-4279 – No connectivity between Brain and AWS after initial setup*
Resolves issue where connectivity between Brain and AWS may fail due proxy misconfiguration after initial setup.

*CS-4356 – Can't backup to S3 bucket*
Resolves issue where 'backup test' command fails when S3 is configured as backup target.

*CS-4300 – Data Smuggler detection contains no details*
Fixes an issue where Data Smuggler detection is not properly bundled and may be missing detection details when only one leg of the detection (push vs pull) is triaged.

*CS-4223 – Triage of SMB Account Scan reports problem calculating impact*
Fixes an issue where the triage of SMB Account Scan returns non-descript error when the source conditions of hosts is above the max payload size.

*CS-4223 – Default vCenter port is incorrectly set to 422*
Resolves UI issue where the default port for vCenter is set to 422 instead of 443.

*CS-4321 – Can't create report if detection type includes any Custom Model*
Resolves issue where report cannot be created if Custom Model is included in detection type.

*CS-4297 – SSL chain certificates for HTTPS/UI does not work*
Resolves issue where input of SSL certificate chain in vsupport CLI may get truncated, causing the certificate chain to become invalid.

*CS-4404 – Syslog CEF host scoring change events are not being forwarded*
Resolves a bug that enables syslog filtering which may prevent host scoring changes to be forwarded from Detect.

*APP-11691 – Legacy CrowdStrike credentials will no longer respect proxy*
Resolves issue where the introduction of OAuth2 credential support for CrowdStrike may cause legacy auth configuration for CrowdStrike to ignore Detect’s proxy configuration.